PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/14 | A2

(11) International Publication Number: **WO 99/41877**

(43) International Publication Date: 19 August 1999 (19.08.99)

(21) International Application Number: PCT/FI99/00113

(22) International Filing Date: 12 February 1999 (12.02.99)

(30) Priority Data:
980339 13 February 1998 (13.02.98) FI

(71) Applicant *(for all designated States except US)*: NOKIA MOBILE PHONES LTD. [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HAKASTE, Markus [FI/FI]; Kuikkarinne 7 B 23, FIN–00200 Helsinki (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN–00101 Helsinki (FI).

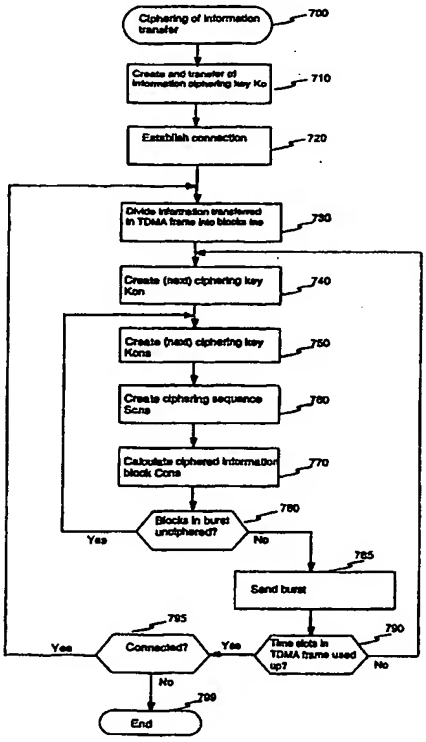
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND ARRANGEMENT FOR CIPHERING INFORMATION TRANSFER

(57) Abstract

The invention relates to a method and arrangement for ciphering an information transfer connection. The invention can be advantageously applied in a TDMA (Time Division Multiple Access) cellular system offering broadband circuit switched services. An essential idea of the invention is that the information to be ciphered in a transmission burst is divided into at least two blocks (730) and said blocks are ciphered in ways that are not identical with each other (750 to 770). Then the reliability of ciphering is better because the amount of information encoded using one and the same ciphering algorithm and key is smaller. In addition, the reliability of the ciphering can be varied by changing the number and/or size of the information blocks in a burst.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method and arrangement for ciphering information transfer

The invention relates to a method and arrangement for ciphering information transfer. The invention can be advantageously applied in a time division multiple access (TDMA) cellular system offering broadband circuit switched services.

The prior art will be now described, discussing first the use of time slots in the GSM (Global System for Mobile communications) system and the coding of information in a burst transferred in a time slot. Then it will be described a known method for ciphering information transfer in said system as well as the disadvantages related to it.

Current mobile communication networks generally use the time division multiple access (TDMA) method. For example, in the GSM system each traffic channel uses TDMA frames comprising eight time slots. In mobile communication systems a call is conventionally established in such a manner that one time slot is reserved for the call and the transmission channel provided by that time slot is then used for the whole duration of the call. If, however, the mobile station moves from the area of a base station to that of another, a handover is carried out and a channel using a new time slot is established between the new active base station and the mobile station.

Fig. 1 shows a GSM TDMA frame comprising eight time slots 0 to 7. Separately shown are transmission frame TX and reception frame RX. Here, transmission frame means a frame sent by the mobile station, i.e. an uplink TDMA frame, and reception frame means a frame received by the mobile station, i.e. a downlink TDMA frame. A cross in Fig. 1 marks the time slot 1 which in the call depicted by the example is used in both uplink and downlink transmission. It should be noted that in the downlink and uplink directions there is a delay between the frames, which is why time slots represented by corresponding numbers are not simultaneous in the different transfer directions.

Broadband high speed circuit switched data (HSCSD) services, in which a call uses more than one time slot in order to speed up the communications rate, have been introduced especially for data transmission services. The number of uplink time slots may be equal to that of downlink time slots, in which case the configuration is symmetrical, or it may be unequal, in which case the configuration is asymmetrical. Time slots used are specified during call establishment and the system indicates the time slots used as well as the related parameters to the mobile station. Said para-

meters include, for example, the ciphering key used in ciphering/deciphering. The number of time slots used can also be changed during a call.

Fig. 2 shows a TDMA frame in conjunction with a HSCSD call using two time slots 1 and 2 in the uplink direction TX and three time slots 0 to 2 in the downlink direction RX.

Fig. 3 illustrates the use of a time slot in the GSM system. A burst transferred in a time slot contains training sequence symbols TSS 33, two sequences IS1 and IS2 consisting of information symbols, 31 and 32, and tail symbols TS1 and TS2, 30 and 34, respectively. In addition, time slots are separated by guard periods GP, 35. A conventional GSM system uses GMSK modulation to modulate the data into the burst.

Furthermore, there are new solutions to increase the transfer capacity by changing the method of modulation of the burst transmitted in a time slot. One such solution is the so-called EDGE (Enhanced Data rates for GSM Evolution) system which is now being developed and is based on the GSM system. In that solution, GMSK modulation may be replaced by binary order quadrature amplitude modulation (B-O-QAM), quadrature order quadrature amplitude modulation (Q-O-QAM) or by code pulse modulation (CPM), for example. Possible characteristics of the EDGE system are described e.g. in [1]. To illustrate the invention we will examine in this patent application some of the arrangements to implement the EDGE system discussed in said document. Those arrangements will be below called the "EDGE system" although the characteristics of the eventual implemented EDGE system might be different from those described here.

When using fast modulation, the symbol rate can be generated from a 13-MHz clock frequency by dividing by 36, for example, while in the conventional GSM system the divisor is 48. Thus the symbol rate becomes 361.111 ksps (kilosymbols per second). When using Q-O-QAM modulation, a symbol comprises 2 bits, so the modulation bit rate is 722.222 kbps (kilobits per second). When using B-O-QAM modulation, a symbol comprises one bit, so the modulation bit rate is 361.111 kbps.

Table 1 below lists the most important modulation characteristics of the GSM system and the system using QAM modulation.

Modulation	GSM	B-O-QAM	Q-O-QAM
Time slot length	576.92 µs	576.92 µs	576.92 µs
Clock frequency divisor	48	36	36
Symbol rate	270.833 ksps	361.111 ksps	361.111 ksps
Symbol sequence length	3.692 µs	2.769 µs	2.769 µs
Modulation bit rate	270.833 kbps	361.111 kbps	722.222 kbps
Symbols in burst	156.25	208.333	208.333
Symbols in TDMA frame	1250	1666.666	1666.666

Table 1

So, using QAM modulation, a burst in one time slot can transfer 208.333 symbols, whereas the GSM system can only transfer 156.25 symbols.

Table 2 below shows the time slot sequence lengths in the GSM system and in the system based on QAM modulation. The portion of the stealing flag is shown separately in the numbers of information symbols and bits.

Modulation	GSM	B-O-QAM	Q-O-QAM
Tail symbols /TS	3	2	2
Information symbols /IS	57 + 1	81 + 1	81 + 1
Information symbols /burst	114 + 2	162 + 2	326 + 2
Symbols in training sequence /TSS	26	28	28
Guard period GP	8.25 (30.462 µs)	12.333 (34.153 µs)	12.333 (34.153 µs)

Table 2

In the GSM system the ciphering of information transferred is based on the use of the so-called A5 ciphering algorithm. The ciphering algorithm is used to produce a 114-bit pseudo-random ciphering sequence which is used to encrypt the 114 information bits transferred in one burst. A ciphered 114-bit sequence is produced by performing an exclusive-or (xor) operation between the unciphered information and the ciphering sequence. Similarly, the ciphered information is deciphered at the

receiving end by producing the same ciphering sequence and carrying out an xor operation between the ciphering sequence and the received bit sequence.

The A5 algorithm is not public but as regards its structure it is a conventional ciphering algorithm using two input parameters. The first input parameter, so-called COUNT value, is derived from the TDMA frame number and transferred on the synchronization channel SCH. The COUNT value is used for producing ciphering blocks for bursts in sequential TDMA frames. The second input parameter is a call specific ciphering key Kc which is transferred on a data transmission channel prior to call establishment.

Different connections and time slots within a TDMA frame are distinguished using separate ciphering keys. If a connection uses more than one time slot, ciphering key Kc is used in time slot 0 if that is in use. In addition, ciphering key Kc is used to produce the ciphering keys Kcn (n = 0 to 7) for the other time slots.

The method above is used for creating for all bursts different ciphering bit blocks within a TDMA frame and between TDMA frames. The use of multiple input parameters in the A5 algorithm makes it possible to avoid long text sequences ciphered with one and the same ciphering block. This way, the encryption function of the conventional GSM system can be made comparatively reliable.

Ciphering methods for the GSM system are described in more detail in [2], chapter 4.

Prior-art arrangements, however, have limitations. The reliability of encryption largely depends on how much information is transferred using the same ciphering algorithm and key. The greater the amount of information transferred using the same algorithm/key, the easier it is to crack the encryption. In known arrangements one and the same ciphering algorithm and key are used to code one burst. When the amount of information in the burst is fixed, the encryption has a certain pre-determined reliability. Thus, known arrangements do not allow selection of the reliability level of encryption according to need.

Also, when using modulation methods in which greater amounts of data are modulated into one burst, the reliability of the encryption becomes lower. A situation may then occur in which the reliability of encryption is inadequate.

Furthermore, known solutions have the disadvantage that when new modulation methods are introduced, longer information blocks and ciphering sequences have to

be handled in conjunction with ciphering, which may call for changes in the transmitter and receiver construction.

An object of the present invention is to avoid aforementioned disadvantages of the prior art by providing an arrangement in which the attainable reliability of encryption is better than in known solutions and in which the level of reliability of encryption can be changed if desired.

An essential idea of the invention is that the information transferred in a burst is divided into at least two blocks and said blocks are ciphered in a non-identical manner. Then the ciphering reliability is better as the amount of information encoded with one and the same ciphering algorithm and key is smaller. Furthermore, the level of ciphering reliability can be changed by altering the number and/or size of information blocks in the burst. Since the information block size can be e.g. 114 bits, which is used in the GSM system, application of the invention will not require that the construction of the mobile station be made more complex.

Fig. 4 shows in general an arrangement according to the invention for ciphering the information related to a burst. A block contains Y information bits of a burst to be ciphered, divided into s+1 sub-blocks each of which comprises y bits. Sub-blocks are created in accordance with predetermined rules. In the example depicted in Fig. 4, the bits to be transferred first are transferred in the first sub-block, the bits to be transferred second are transferred in the second sub-block, etc. However, other ways of forming the sub-blocks can be applied, too. Since in the situation according to Fig. 4 the number of information bits in a burst, i.e. the block size Y, is a multiple of the number of bits y in a sub-block, all sub-blocks are of the same length. A ciphering sequence block 0 to s is formed for each sub-block in a manner described later on. An xor operation is performed between the information bits and ciphering bits, producing Y ciphered information bits for one burst.

Fig. 5 shows a situation in which an information bit block related to a burst, comprising Y bits to be ciphered, is divided into sub-blocks 114 bits long. In this case the block size Y is not a multiple of the number of bits y in a sub-block, so the last sub-block s will not be full. As the number of bits in one burst may not necessarily be divisible by 114, the last sub-block s may comprise less than 114 bits. The remaining bits are the most significant bits of the last sub-block and they are binary added to the corresponding bits of the last ciphering block. The ciphering sequence blocks are generated in the same manner as in the situation depicted in

Fig. 4, producing after an xor operation a block of Y ciphered information bits for one burst.

The method according to the invention for ciphering a TDMA data transfer call, wherein transferred information is modulated into at least one burst of a TDMA frame and transferred information is ciphered using a predetermined algorithm and ciphering key, is characterized in that

- information transferred in one burst is divided into at least two blocks,
- the first block is ciphered using a first ciphering key,
- the second block is ciphered using a second ciphering key, and
- said first and second ciphering keys are different from each other.

The arrangement according to the invention for ciphering a TDMA information transfer connection in a communications system, comprising means for modulating the information to be transferred into at least one burst of a TDMA frame and means for ciphering the information to be transferred using a predetermined algorithm and at least one ciphering key, is characterized in that it further comprises means for dividing the information transferred in said burst into at least two blocks, and means for ciphering the first block using a first ciphering key and the second block using a second ciphering key, said first and second ciphering keys being different from each other.

The mobile station according to the invention, comprising means for ciphering a TDMA information transfer connection, including means for modulating the information to be transferred into at least one burst of a TDMA frame and means for ciphering the information to be transferred using a predetermined algorithm and at least one ciphering key, is characterized in that the mobile station further comprises means for dividing the information transferred in said burst into at least two blocks, and means for ciphering the first block using a first ciphering key and the second block using a second ciphering key, said first and second ciphering keys being different from each other.

Preferred embodiments of the invention are described in the dependent claims.

Embodiments of the invention will now be described in more detail with reference to the accompanying drawing wherein

Fig. 1 shows the allocation of a time slot in a TDMA frame in a conventional connection using one time slot,

Fig. 2 shows the allocation of time slots in a TDMA frame in a HSCSD connection using multiple time slots,

Fig. 3 illustrates time slot usage in the GSM system,

Fig. 4 illustrates in accordance with the invention ciphering of information encoded into a burst when the burst comprises an evenly divisible number of information blocks,

Fig. 5 illustrates in accordance with the invention ciphering of information encoded into a burst when the number of information blocks in the burst is not an evenly divisible figure,

Fig. 6 shows in the form of flow diagram a method according to the invention for ciphering information transfer when the connection uses one time slot,

Fig. 7 shows in the form of flow diagram a method according to the invention for ciphering information transfer when the connection uses multiple time slots, and

Fig. 8 shows in the form of block diagram a mobile station according to the invention and its connection to a cellular system.

Figs. 1 to 3 were already discussed above in conjunction with the description of the prior art, and Figs. 4 and 5 were discussed in conjunction with the general description of the invention.

Referring to Fig. 6, it will be now described in more detail a method according to the invention for ciphering information transfer on a communications connection using one time slot, and referring to Fig. 7, it will be described a method according to the invention for a communications connection using multiple time slots. Then, referring to Fig. 8, it will be described an arrangement for realizing a mobile station according to the invention.

Fig. 6 shows a method according to the invention for ciphering a connection using one time slot, 600. First, a connection specific ciphering key Kc is created and transferred on the information transfer channel so that both the transmitter and receiver use the same connection key, step 610. In conjunction with that, normal call establishment is carried out, step 620. Information to be transferred is divided into blocks the size of which in the example case is 114 bits, step 630.

Next, a block specific ciphering key Kcs is created in step 650. The first 114-bit block is advantageously encoded using the same ciphering sequence as in the normal single-slot case because Kc0 = Kc. For all subsequent sub-blocks 1 to s it is

used distinct ciphering sequences derived from the corresponding connection specific ciphering keys Kc1 to Kcs.

The block specific ciphering key is created using the connection specific ciphering key Kc and the sub-block number BM as follows:

$$Kcs(i) = Kc(i)\ xor\ BMs(i) \quad (1)$$

In the equation above, xor stands for bitwise binary addition. BM(i) stands for 64-bit binary encoding of the sub-block number BM. The sub-block number may obtain values in the range 0 to DIV(Y,114), where Y is the total number of information bits to be ciphered in one burst, i.e. the block size. Index s denotes the sub-block index and i denotes binary form.

In a system using the new modulation method the number of information bits to be ciphered in the burst is advantageously 200 to 400. If the number of bits to be ciphered is e.g. 300, the number of sub-blocks is DIV(300,114) = 2. Then the sub-block numbers 0, 1 and 2 are binary-encoded such that the bit sequence contains 62 zeros followed by the two least significant bits, which have the value 00, 01 or 10, depending on the sub-block.

Using a block specific ciphering key, a block specific ciphering sequence Scs is created, step 660. After that, an information sub-block is ciphered using the ciphering sequence block, producing a ciphered information block Ccs.

If there are still information blocks in the burst to be ciphered, operation returns to step 650. When all information blocks in the burst have been ciphered, 680, the ciphered information blocks are modulated into the burst and the burst is transmitted to the information transfer channel, step 685. Steps 630 to 685 are continued until the connection is terminated, 699.

A received burst is decoded following corresponding deciphering steps.

Fig. 7 shows a ciphering method 700 according to the invention in which information transfer in the HSCSD case uses one or more time slots of a TDMA frame. Here, too, a connection specific ciphering key Kc is created first, step 710. After the call has been established, 720, information in each time slot is divided into blocks Ins, step 730. Then, in step 740, a time slot specific ciphering key Kcn is created, where n stands for the number of the time slot in the TDMA frame. The ciphering

key Kcn is generated using the connection specific ciphering key Kc and time slot number BN as follows:

$$Kcn(i) = Kc(i)\ xor\ (BN << 32(i)) \quad (2)$$

In equation (2), operation <<32 represents a 32-bit shift.

Then, in step 750, a new connection specific ciphering key Kcns is created for the information block in the burst on the basis of the sub-block number BM as follows:

$$Kcns(i) = Kcn(i)\ xor\ BMs(i) \quad (3)$$

As mentioned above in conjunction with the description of Fig. 6, xor stands for bitwise binary addition and BM(i) stands for binary encoding of the value of the sub-block number BM into 64 bits. It should be noted here that the time slot number should be indicated using a different part of the bit sequence than that used to indicate the time slot number in the HSCSD solution, lest the effect of the parameters in the multichannel case be canceled. Namely, if the bits in question are summed at the same point of the bit sequence, the reliability of encryption might be degraded because the time slot number and sub-block number are data that a third party could find out. In the HSCSD solution in use, the bits indicating the time slot are situated in the middle of the 64-bit sequence.

The ciphering key produced is used to generate a block specific ciphering sequence Scns in step 760 which is used to calculate the ciphered information block Ccns, step 770. Steps 750 to 770 are repeated until all information blocks in the burst have been ciphered, 780, whereafter the burst is generated and transmitted, 785. Correspondingly, steps 740 to 785 are repeated until all bursts of the time slots used by the connection have been ciphered and transmitted, 790, after which the operation returns 795 to step 730 until the connection is terminated, 799.

Also in the case of a multislot connection, the deciphering in the reception is carried out according to steps corresponding to those used in the ciphering in the transmission.

Fig. 8 shows in the form of a simplified block diagram a mobile station 800 according to the invention and its connection to a cellular system. The mobile station comprises an antenna 801 to receive a radio-frequency, or RF, signal sent by a base station. The received RF signal is taken e.g. by means of a duplex filter or switch 802 to a RF receiver 811 where the signal is amplified and converted digital. Then

the signal is detected and demodulated in block 812. Block 813 performs deciphering according to the present invention as well as deinterleaving. Signal processing is then performed in block 830 according to whether the information transferred is speech or data. Data can be stored as such in the mobile station's memory 804 or, alternatively, processed data are transferred after signal processing to a possible external device such as a computer. Possible processed speech signal is taken to an earphone (not shown). A control unit controls aforementioned receiving blocks in accordance with a program stored in the unit. The control unit controls block 813 in such a manner that deciphering of data received from the system is carried out as described above.

Transmission from a mobile station in accordance with the invention is carried out e.g. as follows. Controlled by a control unit 803, block 833 performs the signal processing and block 821 performs the interleaving and ciphering according to the invention for the processed signal (data/speech) to be transferred. Bursts are generated from the encoded data in block 822 which are modulated and amplified into a transmission RF signal, block 823. The RF signal to be transmitted is taken to an antenna 801 via a duplex filter 802, for example. Also the aforementioned processing and transmission functions are controlled by a control unit 803. Especially the control unit controls block 821 in such a manner that the information in each burst is ciphered according to the invention using separate ciphering sequences for each information block. To that end, the control unit reads from the memory 804 the necessary ciphering parameters. In addition, the control unit 803 monitors the SCH channel to receive the COUNT value. The COUNT value is received at the beginning of the connection or when the synchronization is restored after a visit outside the coverage area or in connection with a handover.

In addition, Fig. 8 shows a keypad 831 and display 832 belonging to a normal mobile station. Blocks of a mobile station according to the invention can be formed using known components. However, the control unit controlling the other units carries out the block control functions in accordance with special software, thus realizing the aforementioned block functions according to the invention.

Furthermore, Fig. 8 shows the parts of the cellular system that are used in the call establishment and information transfer. RF signal transmission and reception are carried out through an antenna 850 in a base station 851. An information transfer connection is created from the base station 851 via a base station controller 852 to a switching center 853. In addition to other base station systems of the system, the

switching center 853 is connected to a home location register 854 and public switched telephone network PSTN, for example.

On the communications system side, the ciphering and deciphering according to the invention are performed at a base station by means of blocks corresponding to those of a mobile station.

It should be noted that in the downlink and uplink directions of a connection it is possible to use different time slot numbers as well as different ciphering and modulation methods. In addition, the number of time slots used, the size/number of information blocks in a burst and the modulation method can be changed also during the connection.

Above the invention was described using certain embodiments as examples. It is however obvious that the invention is not limited to those embodiments but can be freely modified within the limits defined by the claims set forth below.

It should be especially noted that the invention is not limited to the GSM system but can be well applied to other systems using the TDMA method and also systems using the code division multiple access, or CDMA, method. Similarly, the invention is not limited to the modulation methods mentioned above but it can be applied in conjunction with other modulation methods, too. Furthermore, the invention is not limited to data transfer but can be applied to the transfer of speech as well. The invention also comprises ciphering on those signalling channels where new modulation might be needed. Such channels in the GSM/EDGE system could be e.g. the fast associated control channel FACCH, as well as the SACCH and SDCCH channels. Furthermore, configurations more complex than those described can occur in various situations within the scope of the principle of the invention.

References

[1] ETSI STC SMG2 EDGE Tdoc 332/97: Feasibility Study version 1.0, Work Item 184: Improved Data Rates through Optimised Modulation, Ericsson, Nokia, December 1-5, 1997.

[2] Draft ETS 300 929: GSM 03.20 - version 5.1.0. Digital cellular telecommunications system (phase 2+); Security related network functions, European Telecommunications standards Institute, March 1997, 51 pp.

Claims

1. A method for ciphering a communications connection wherein information to be transferred is modulated into at least one burst and the information to be transferred is ciphered according to a predetermined algorithm and ciphering key, **characterized** in that
- information transferred in one burst is divided into at least two blocks,
- the first block is ciphered using a first ciphering key (Kcn1),
- the second block is ciphered using a second ciphering key (Kcn2), and
- said first and second ciphering keys are different from each other.

2. The method of claim 1, **characterized** in that the size (y) of said block is substantially smaller than the amount of information (Y) transferred in one burst.

3. The method of claim 1 or 2, **characterized** in that the number (s) of information blocks transferred in a burst is changed during the connection.

4. The method of any one of the preceding claims, **characterized** in that the size (y) of the information blocks transferred in a burst is changed during the connection.

5. The method of any one of the preceding claims, **characterized** in that said ciphering key (Kcns) is generated on the basis of a parameter (COUNT) transferred on an information transfer channel.

6. The method of any one of the preceding claims, **characterized** in that said information transfer connection substantially complies with the EDGE system.

7. An arrangement for ciphering an information transfer connection in a communications system, said arrangement comprising means for modulating the information to be transferred into at least one burst and means for ciphering the information to be transferred by means of a predetermined algorithm and at least one ciphering key, **characterized** in that it further comprises means for dividing the information transferred in said burst into at least two blocks, and means for ciphering the first block using a first ciphering key and the second block using a second ciphering key, said first and second ciphering keys being different from each other.

8. A mobile station comprising means for ciphering an information transfer connection, said means including means for modulating the information to be transferred into at least one burst and means for ciphering the information to be

transferred by means of a predetermined algorithm and at least one ciphering key, **characterized** in that the mobile station further comprises means for dividing the information transferred in said burst into at least two blocks, and means for ciphering the first block using a first ciphering key and the second block using a second ciphering key, said first and second ciphering keys being different from each other.

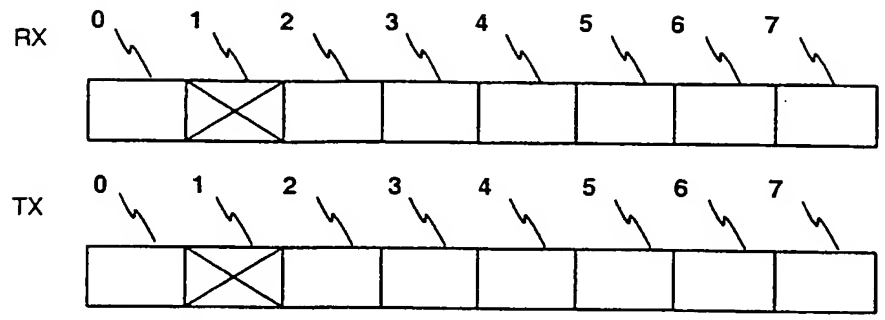


FIG 1.

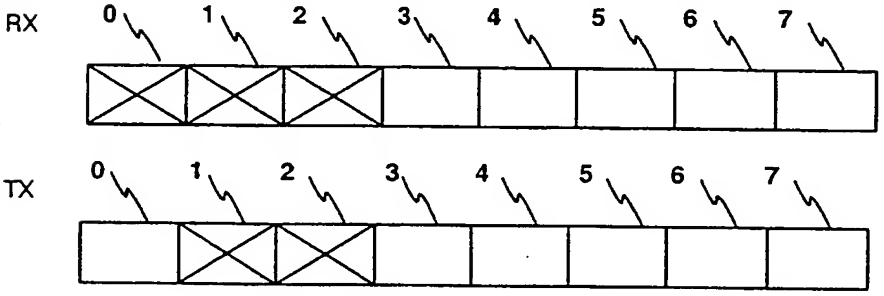


FIG 2.

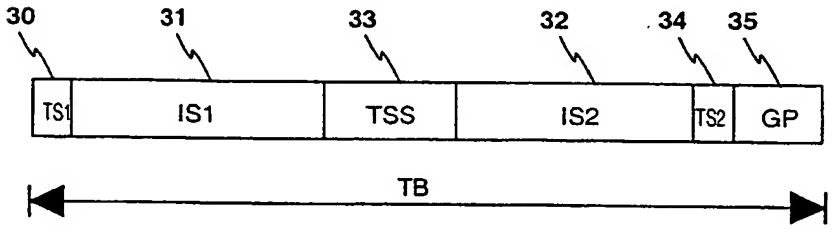


FIG 3.

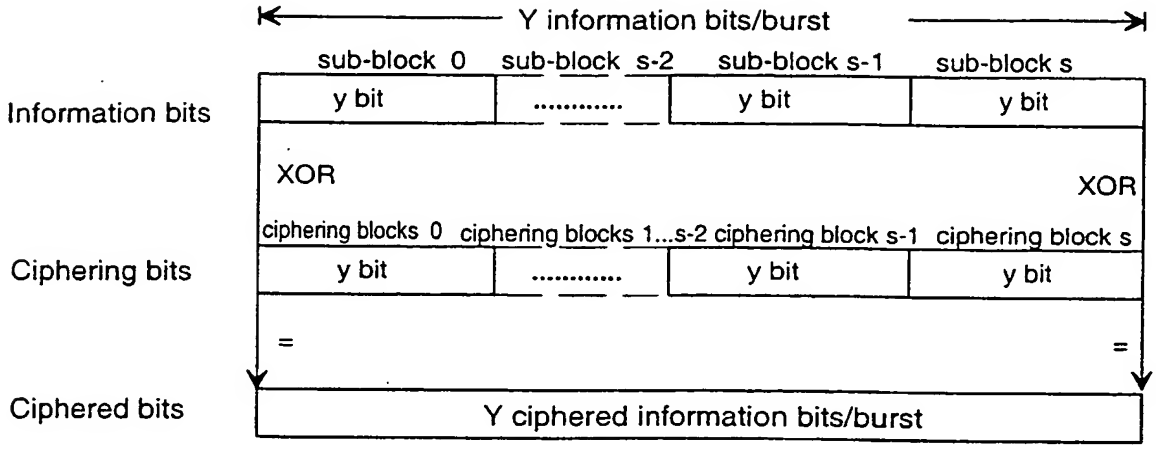

Y information bits/burst
sub-block 0
sub-block s-2
sub-block s-1
sub-block s
Information bits
y bit
.....
y bit
y bit
XOR
XOR
ciphering blocks 0
ciphering blocks 1...s-2
ciphering block s-1
ciphering block s
Ciphering bits
y bit
.....
y bit
y bit
=
=
Ciphered bits
Y ciphered information bits/burst

FIG 4.

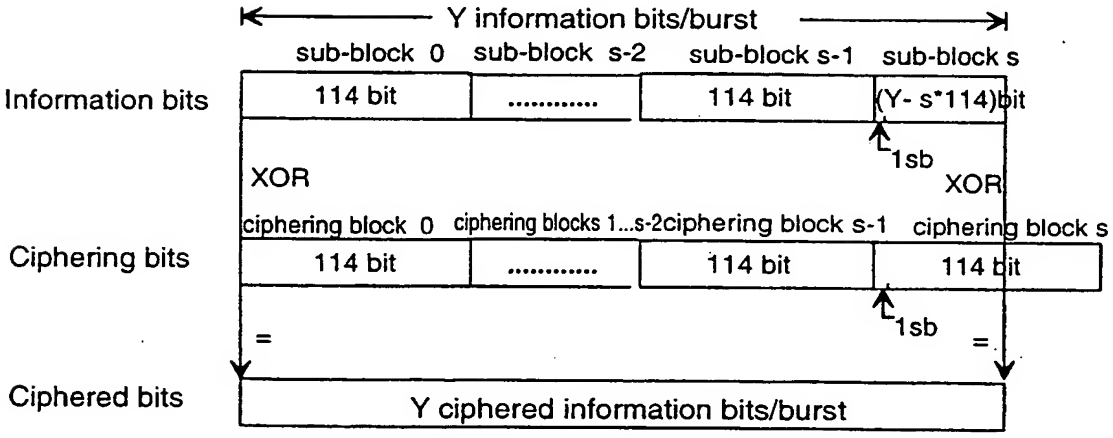

Y information bits/burst
sub-block 0
sub-block s-2
sub-block s-1
sub-block s
Information bits
114 bit
.....
114 bit
(Y- s*114)bit
1sb
XOR
XOR
ciphering block 0
ciphering blocks 1...s-2
ciphering block s-1
ciphering block s
Ciphering bits
114 bit
.....
114 bit
114 bit
1sb
=
=
Ciphered bits
Y ciphered information bits/burst

FIG 5.

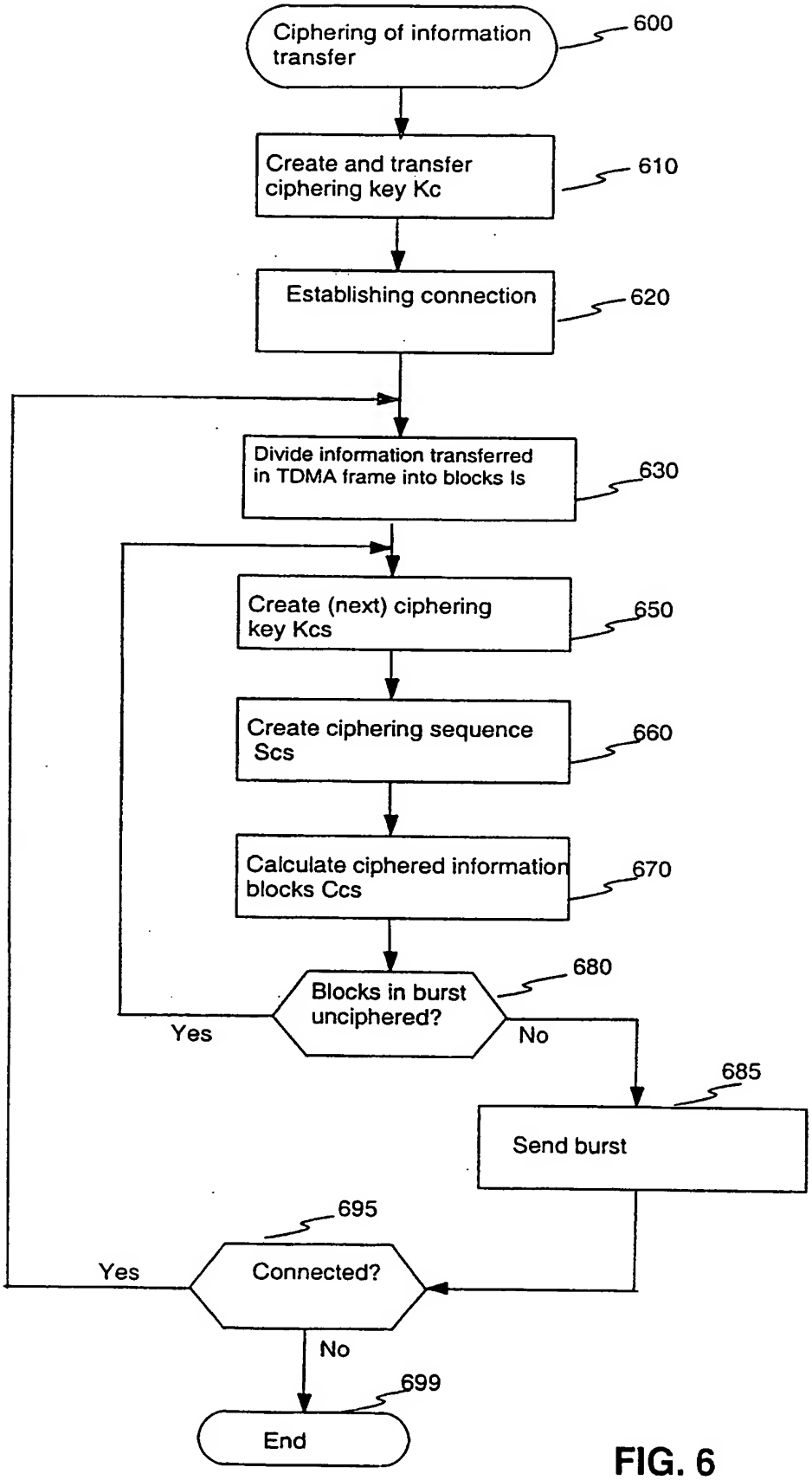

Ciphering of information transfer
600
Create and transfer ciphering key Kc
610
Establishing connection
620
Divide information transferred in TDMA frame into blocks Is
630
Create (next) ciphering key Kcs
650
Create ciphering sequence Scs
660
Calculate ciphered information blocks Ccs
670
Blocks in burst unciphered?
680
Yes
No
Send burst
685
Connected?
695
Yes
No
End
699

FIG. 6

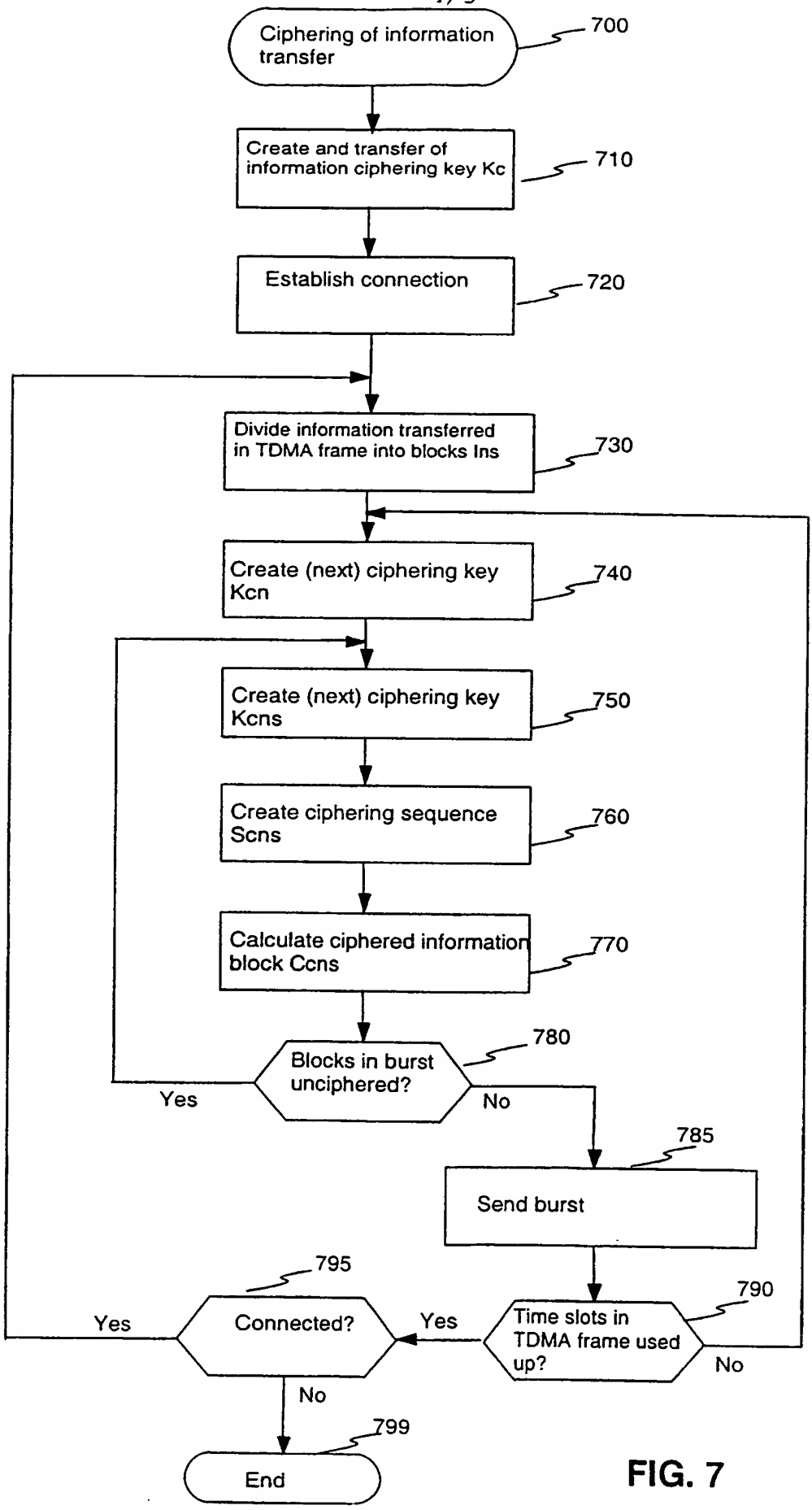

Ciphering of information transfer
700
Create and transfer of information ciphering key Kc
710
Establish connection
720
Divide information transferred in TDMA frame into blocks Ins
730
Create (next) ciphering key Kcn
740
Create (next) ciphering key Kcns
750
Create ciphering sequence Scns
760
Calculate ciphered information block Ccns
770
Blocks in burst unciphered?
780
Yes
No
Send burst
785
Time slots in TDMA frame used up?
790
Yes
No
Connected?
795
Yes
No
End
799

FIG. 7

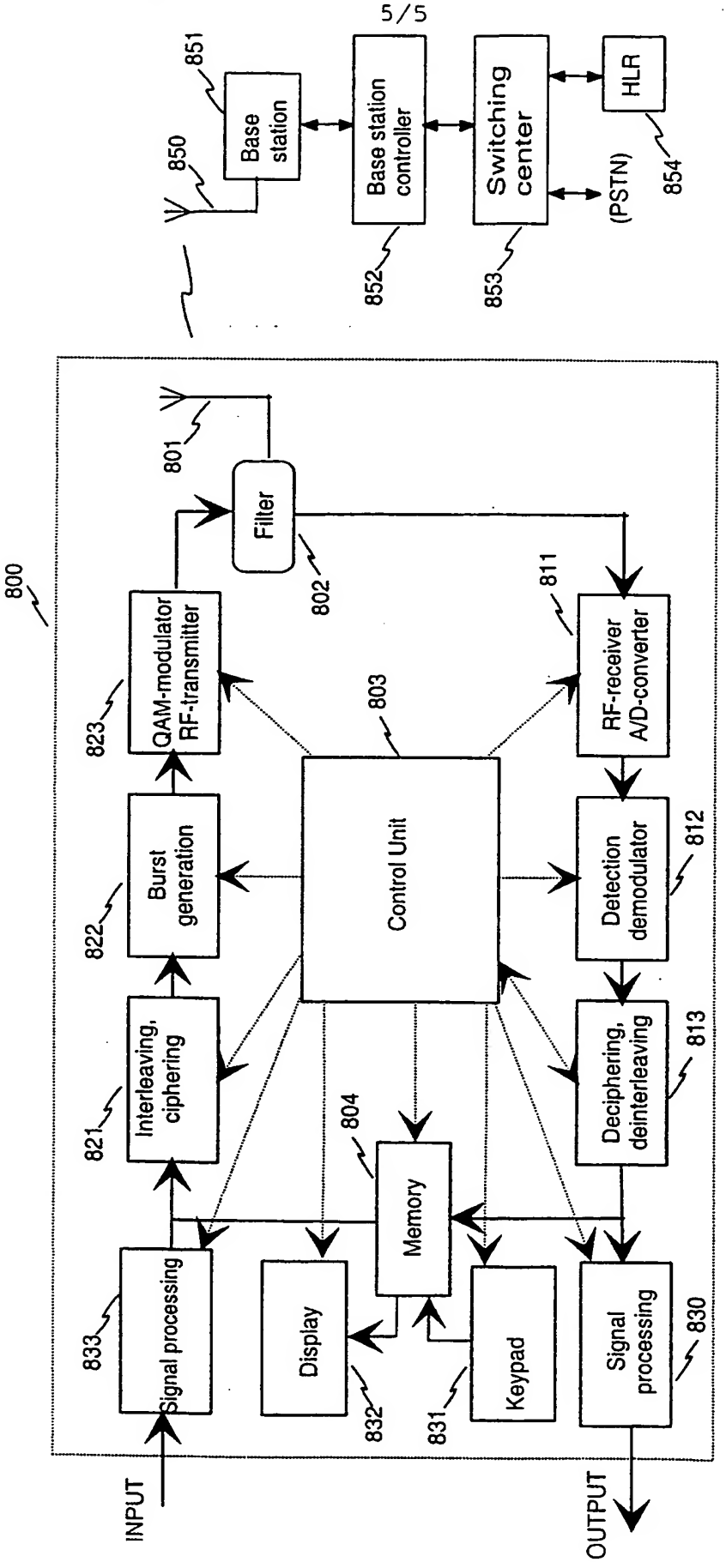

851
Base station
850
Base station controller
852
Switching center
853
HLR
854
(PSTN)
800
801
Filter
802
811
RF-receiver A/D-converter
QAM-modulator RF-transmitter
823
803
Control Unit
Burst generation
822
Detection demodulator
812
Interleaving, ciphering
821
804
Memory
Deciphering, deinterleaving
813
Signal processing
833
Display
832
Keypad
831
Signal processing
830
INPUT
OUTPUT

FIG. 8

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/14

A3

(11) International Publication Number: WO 99/41877

(43) International Publication Date: 19 August 1999 (19.08.99)

(21) International Application Number: PCT/FI99/00113

(22) International Filing Date: 12 February 1999 (12.02.99)

(30) Priority Data:
980339 13 February 1998 (13.02.98) FI

(71) Applicant *(for all designated States except US)*: NOKIA MOBILE PHONES LTD. [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HAKASTE, Markus [FI/FI]; Kuikkarinne 7 B 23, FIN–00200 Helsinki (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN–00101 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

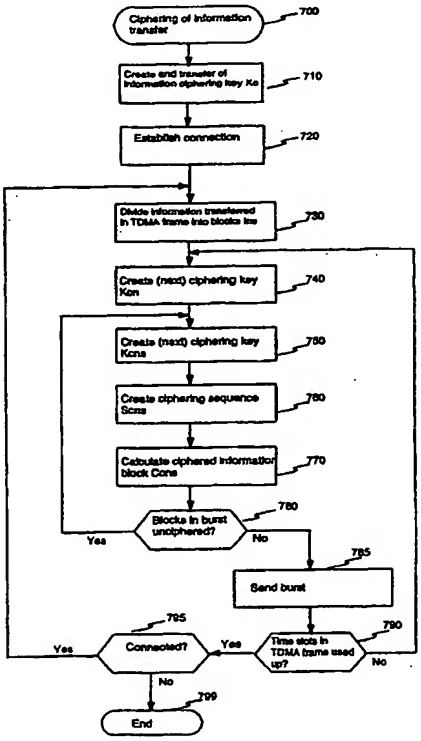
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
30 September 1999 (30.09.99)

(54) Title: METHOD AND ARRANGEMENT FOR CIPHERING INFORMATION TRANSFER

(57) Abstract

The invention relates to a method and arrangement for ciphering an information transfer connection. The invention can be advantageously applied in a TDMA (Time Division Multiple Access) cellular system offering broadband circuit switched services. An essential idea of the invention is that the information to be ciphered in a transmission burst is divided into at least two blocks (730) and said blocks are ciphered in ways that are not identical with each other (750 to 770). Then the reliability of ciphering is better because the amount of information encoded using one and the same ciphering algorithm and key is smaller. In addition, the reliability of the ciphering can be varied by changing the number and/or size of the information blocks in a burst.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00113

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/14
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9800949 A1 (TELEDYNE INDUSTRIES INC.), 8 January 1998 (08.01.98), page 1, line 10 - line 13, abstract	1-2,7
A		3-6,8
	--	
X	US 5638445 A (JEFFREY F. SPELMAN ET AL), 10 June 1997 (10.06.97), abstract	1-2,7
A		3-6,8
	--	
A	WO 9510906 A1 (IRDETO B.V.), 20 April 1995 (20.04.95), abstract	1-8
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 July 1999	04 -08- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00113

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9118460 A1 (TRAUTNER, ROLF), 28 November 1991 (28.11.91), abstract --	1-8
A	US 5511123 A (CARLISLE M. ADAMS), 23 April 1996 (23.04.96), abstract --	1-8
A	GB 2264373 A (EUROLOGIC RESEARCH LIMITED), 25 August 1993 (25.08.93), abstract --	1-8
A	EP 0518315 A2 (MITSUBISHI DENKI KABUSHIKI KAISHA), 16 December 1992 (16.12.92), abstract -- --------	1-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/07/99

International application No.
PCT/FI 99/00113

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9800949 A1	08/01/98	US 5778074 A	07/07/98
US 5638445 A	10/06/97	US 5761311 A	02/06/98
		US 5764768 A	09/06/98
WO 9510906 A1	20/04/95	AT 176970 T	15/03/99
		AU 683325 B	06/11/97
		AU 1078395 A	04/05/95
		DE 69416684 D	00/00/00
		EP 0723726 A,B	31/07/96
		SE 0723726 T3	
		NL 9301784 A	01/05/95
		US 5799089 A	25/08/98
		ZA 9407822 A	12/07/95
WO 9118460 A1	28/11/91	DE 4016203 A	21/11/91
US 5511123 A	23/04/96	CA 2134410 A,C	05/02/96
		JP 8063097 A	08/03/96
GB 2264373 A	25/08/93	NONE	
EP 0518315 A2	16/12/92	DE 69222090 D,T	26/03/98
		JP 2862030 B	24/02/99
		JP 4365240 A	17/12/92
		US 5261003 A	09/11/93
		US 5488661 A	30/01/96